REMARKS

Applicant respectfully requests reconsideration of this application, as amended, and consideration of the following remarks. Claims 1, 7, 12, 14, 18, and 19 have been amended. Claim 16 was previously canceled. Claims 5, 6, 11, 13, 15-17, has been canceled. Claims 1-4, 7-10, 12, 14 and 18-20 remain pending. Claims 1-10, 12 and 14-20 stand rejected under 35 U.S.C. 103(a).

Amendments

Amendments to the Claims

Applicant has amended the claims to more particularly point out what Applicant regards as the invention. No new matter has been added as a result of these amendments.

Rejections

Rejections under 35 U.S.C. §103(a)

Claims 1-10, 12 and 14-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Anand (US Pat Pub 2002/0191792, now issued as US Pat 7,213,148) in view of Dworkin (US Pat 7,142,669). Applicant respectfully traverses these rejections as set forth in more detail below.

The Anand reference discloses a hash processing system and method for reducing the number of clock cycles required to implement the SHA1 and MD5 hash algorithms by using a common hash memory having multiple storage areas each coupled to one of two or more hash channels. The system further provides implicit padding on-the-fly as data is read from the common hash memory. The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel, and uses pipelined, two-channel SHA1 and pipelined, single-channel MD5 hash architectures to reduce the effective time required to implement the SHA1 and MD5 algorithms.

Anand does not share components such as adders or compressors between the different hash circuits. Anand provides completely separate logic circuits to process

each of the different types of hash functions (e.g., the circuit of Fig. 3 to perform a SHA-1 function, the circuit of Fig. 4 to perform an MD5 function) (col. 10, lines 6-10). Anand does share input and output registers for temporary storage of the data being processed by the different hash logic circuits. Sharing the input and output registers is not the same as sharing components within the actual hash function circuits 114, 116 because Anand uses each of the different hash function circuits ***in parallel*** and therefore ***cannot share*** hash functional components ***and maintain parallel function*** capability.

Anand teaches completely separate adders for each hash function and does not disclose shared adders nor systems and methods of selecting the shared adders as claimed by Applicant. It would not be obvious to modify Anand as the separate hash circuits are typically functional blocks that are simply repeated to increase speed (e.g., parallel processing as described by Anand) and in a parallel processing circuit, the adders could not be shared and still maintain full parallel functionality. None of the other cited references correct this deficit in Anan.

The Dworkin reference teaches a Message Digest Hardware Accelerator (MDHA) 10 for implementing multiple cryptographic hash algorithms such as the Secure Hashing Algorithm 1 (SHA-1), the Message Digest 4 (MD4) algorithm and the Message Digest 5 (MD5) algorithm. A register file (12) is initialized to different data values. A function circuit (22) performs logical operations based on the selected algorithm and provides a data value to a summing circuit (30) that is summed with mode dependent constant values selected from registers (34 and 36), round and step dependent data words generated by a register array block (32) to calculate the hash value for a text message stored in registers (100 115).

Referring now to Dworkin's first claim (which all the others are dependent upon) requires the first multiplexer (24) produce the E value for SHA1 and zero for MD5 and that the output of this first multiplexer be input to the summing circuit (30). This summing circuit (30) is a five input summing circuit (see Dworin Figure 1).

This is a substantially different from Applicant's invention. Applicant's first summing circuit is a four input summing circuit (808 and 810).

Further, the SHA1 chaining variable "E" is coupled through Applicant's mux 816, is not added in until the second summing circuit 820.

While Dworkin has two summing circuits, Dworkin's first summing circuit is a five input and the second is a two input. In contrast to Applicant's first summing circuit that is a four input and the Applicant's second summing circuit that is a two input.

Dworkin's five input summing circuit is slower and takes substantially more area than Applicant's four input summing circuit.

Further, since Applicant does not include the E value in the first summing circuit as Dworkin requires.

Further, neither Dworkin nor Anand teach or suggest SHA256, SHA384, or SHA512 hash algorithms. The claims and description of Anand are primarily concerned with the data movement and with efficient SHA1 implementation. The claims and description of Dworkin are limited to SHA1 and MD5.

Applicant structure is not limited to SHA1 and MD5.

As to claims 1-4, 7-10, 12, 14 and 18-20, none of the cited references whether considered alone or in combination teach or suggest a system method or apparatus where the hash modules share logic components (e.g., adders, compressors, etc.) that are selectable and used to perform the respective hash functions. Accordingly, Applicant respectfully submits that Applicant's invention as claimed in claims 1-4, 7-10, 12, 14 and 18-20 is patentably distinct over any of the cited references whether considered alone or in any combination, and respectfully request the withdrawal of the rejections under 35 U.S.C. §103(a).

SUMMARY

In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact George B. Leavell at (408) 749-6900, ext 6923.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 50-0805 (Ref SUNMP349) for any charges that may be due or credit our account for any overpayment. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

MARTINE PENILLA & GENCARELLA, LLP

Dated: November 13, 2007

George B. Leavell
Attorney for Applicant
Registration No. 45,436

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
(408) 749-6900 ext 6923